REMARKS

The final Office Action dated January 14, 2005 has been received and carefully considered. The above amendments and the following remarks are being submitted as a full and complete response to the Office Action. No new matter has been entered.

In the current Office Action, claims 1-13, 17, 18, 20, 21, 23, 24, 28 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Escamillia in view of Cheswick.

In the Examiner's response to the applicant's arguments, particularly referring to the paragraph bridging pages 2 and 3 of the Office Action, the Examiner appears to acknowledge that Escamillia and Cheswick do not teach closing a gateway to malicious IP packets only for a predetermined amount of time. However, the Examiner contends that the combination of references does teach blocking communication to a network through a firewall. Further, the Examiner contends that, as broadly stated in the claims, the "predetermined time" could imply an open-ended interval, since there was no explicit mention in the claims that the gateway should be reopened after the period has ended.

Directly in response to the Examiner's suggestion, claims 1 and 28 have now been amended to more clearly state that the *gateway is reopened* after the predetermined time has elapsed. More specifically, as presently amended, claims 1 and 28 state that the processing means comprises means both for a) preventing an IP packet having a source IP address and/or a destination IP address associated with the attack detected by the attack detecting means from entering the network for a predetermined

time and, when the predetermined time has elapsed after the detecting means detects the attack, b) reopening the gateway for allowing an IP packet having a source IP address and/or a destination IP address associated with the attack to enter the network.

As currently amended, the claimed predetermined time period cannot possibly imply an open-ended interval and, as now amended, there is a clear and explicit mention in the claims that the *gateway is reopened* after the period has ended.

Moreover, it is respectfully submitted that the amendments have been made directly in response to a suggestion from the Examiner, namely, that the claim language was not sufficiently clear to preclude an open-ended time period. Therefore, since the current amendments merely "adopt examiner suggestions," and should require only a cursory review by the Examiner, entry of the amendments is proper. See, MPEP §§ 714.12 and 714.13.

Further, should a showing under 37 CFR § 1.116(b) be required, as to why the amendments are necessary and were not earlier presented, the applicant respectfully submits that, in ordinary usage, the phrase "for a predetermined time" implies a finite time period, and that obviously reopening of the gateway after elapse of the predetermined time was inherent and self-evident in the previous claim language, particularly when considered in light of the arguments that accompanied the previously amended claims. The Examiner's requirement for greater clarity in the claims is, of course, appreciated and the applicant is most willing to meet this requirement. However, the

previous amendments were reasonably believed to be commensurate with the applicant's arguments. Since the current amendments are not only in response to the Examiner's suggestions, but are also clearly in line with arguments already made in the present application, the amendments do not introduce any "new issues" and hence the applicant is entitled to entry of the amendments.

Accordingly, entry of the amendments is respectfully requested. Further, for the reasons already discussed in the applicant's previous response, the claimed invention is not obvious over the cited prior art.

As argued in the applicant's previous response, the full content of which is expressly incorporated herein by reference, according to the claimed invention, once an attack is detected from among stored IP packets, only then the IP packets associated with the attack are prevented from entering the gateway, and only then for a predetermined period of time. Moreover, as set forth in the dependent claims and in claim 28, the predetermined time period may depend, in a flexible manner, on the type of attack. Thus, unlike traditional firewall protections, IP packets associated with the attack are not shut off completely, but rather, the ingress of the IP packets is prevented for a predetermined time period sufficient to stop the attack, and thereafter, the gateway is reopened.

More specifically, the present invention recognizes that IP packets having given destination/source addresses may be used at times for mounting malicious cracker attacks. However, at other times, well-intentioned users can use the same IP packets bearing

the same source/destination addresses without malice. Thus, it is overly restrictive to continuously prohibit access at the gateway to such IP packets. Rather, according to the claimed invention, such IP packets are prevented from passing the gateway only for a sufficient period of time to prevent success of the attack. Once the threat of attack is abated, then the gateway is reopened to such IP packets.

Therefore, contrary to the traditional firewall prevention suggested in the cited prior art, which simply prevents ingress at all times of potentially malicious IP packets through a gateway, the present invention provides a flexible and adaptive technique, which monitors IP packets in a stored location while keeping the gateway open to traffic. When an attack is detected, the gateway is then shut down to prevent ingress of IP packets mounting the attack, but only for a predetermined period of time sufficient to prevent the attack, and thereafter, the gateway is reopened to such IP packets. Thus, the goal of the invention is to enable the gateway to remain open to all traffic, to the greatest extent possible, while still preventing cracker attacks during times when the attacks are being mounted.

In addition to claim 1, independent claim 28 includes the same features discussed above. In particular, according to claim 28, acquired and stored IP packets are monitored while the gateway remains open, to detect cracker attacks from the acquired and stored IP packets based on an algorithm, and IP packets are prevented from entering the network according to a predetermined process, for a time which is predetermined corresponding to the

detected type of attack, after the attack detecting means detects one of the attacks. Again, once the threat of attack is abated, the gateway is reopened to such IP packets. Accordingly, claim 28 is allowable over the cited prior art, essentially for the same reasons as claim 1.

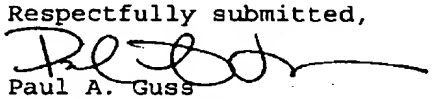
It is respectfully submitted that the cited prior art provides no suggestion for the features of the claimed invention, and does not enable the advantages highlighted above.

As noted previously, there is no discussion whatsoever, in either Escamillia or Cheswick, of storing IP packets that have passed through a gateway, monitoring the IP packets at a stored location remote from the gateway while the gateway remains open, and then preventing an IP packet from entering the network only for a predetermined time, after which the gateway is reopened and access to the network for such IP packets is again permitted.

Accordingly, the applicant respectfully submits that the claimed invention is both novel and non-obvious over the cited prior art. Reconsideration and withdrawal of the rejections is requested.

A petition to extend the response period for replying to the Office Action for three months, until July 14, 2005, accompanies this response. No other fees are due at this time. Notwithstanding, should it be deemed that other fees, or deficiencies in fees, are required in connection with this or any accompanying communication, such amounts may be charged to the Attorney's Deposit Account No. 07-2519.

Respectfully submitted,



Paul A. Guss
Reg. No. 33,099
Attorney for Applicants

CS-02-000131

775 S. 23rd St. #2
Arlington, VA 22202
Tel. 703-486-2710